Date of Hearing: August 30, 2008

ASSEMBLY COMMITTEE ON JUDICIARY
Dave Jones, Chair
AB 1656 (Jones) – As Amended: August 6, 2008

FOR CONCURRENCE

SUBJECT: PERSONAL INFORMATION: SECURITY BREACHES

KEY ISSUES:

1) SHOULD AN ENTITY THAT ACCEPTS CREDIT AND DEBIT CARDS AS PAYMENT BE PROHIBITED FROM STORING, RETAINING, SENDING, OR FAILING TO LIMIT ACCESS TO A CUSTOMER'S PAYMENT-RELATED DATA, SUBJECT TO CERTAIN BUSINESS-RELATED EXCEPTIONS?

2) SHOULD CALIFORNIA'S BREACH NOTIFICATION LAW BE AMENDED SO THAT THE REQUIRED NOTICE CONTAINS SPECIFIED AND USEFUL INFORMATION?

3) WHEN SUBSTITUTE NOTICE IS REQUIRED UNDER THE BREACH NOTIFICATION LAW, SHOULD NOTICE ALSO BE SENT TO THE OFFICE OF INFORMATION SECURITY AND PRIVACY PROTECTION SO THAT THE STATE MIGHT BETTER TRACK BREACH EVENTS?

SYNOPSIS

This bill would, subject to certain exceptions, prohibit a business or entity that accepts credit or debit cards be prohibited from storing, retaining, sending, or allowing unauthorized access to a customer's payment-related information, except for legitimate business purposes. In addition, the bill would strengthen California's data breach notification law by requiring that the breach notice contain specified information and, under certain circumstances, that a copy of the notice be sent to the state Office of Security and Privacy Protection. This bill follows last year's AB 779 (Jones), which was prompted in part by several substantial and well-publicized examples of data breaches that compromised the payment-related data of millions of consumers, including credit card and debit card numbers. Although AB 779 passed out of both houses last year with overwhelming (nearly unanimous) bipartisan support, that measure was vetoed by the Governor. The author contends that he has addressed the concerns raised in the veto message with amendments that, among other things, permit storage of data for the sole purpose of processing on-going and recurring payments, permit notices to contain a "date range" instead of an exact date of breach and discovery, and remove provisions that would have required the business that held that data at the time of breach to reimburse the financial institution for the costs of sending notification. It is not entirely clear whether these amendments will address the Governor's concerns, but the bill is substantially different from last year's AB 779 even as it seeks the same ends. The bill is sponsored by the California Credit Union League and supported by consumer and law enforcement groups.

SUMMARY: Prohibits a person, business, or agency that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device, from

storing, retaining, sending, or failing to limit access to payment-related data, retaining a primary account number, or storing sensitive authentication data subsequent to an authorization, unless a specified exception applies.

The Senate amendments delete the Assembly version of this bill, change the author, and instead:

1) Provide that a person, business, or agency, that sells goods or services to any resident of California and accepts as payment a credit card, debit card, or other payment device shall not do any of the following:

    a) Store payment-related data, except when the person, business, or agency complies with both of the following:

        i) The person, business, or agency shall have a payment data retention and disposal policy that limits the amount of payment-related data and the time that data is retained to only the amount and time required for business, legal, or regulatory purposes as explicitly documented in the policy; and,

        ii) The person, business, or agency shall retain payment-related data only for a time period and in a manner explicitly permitted by the policy.

    b) Store sensitive authentication data, as defined subsequent to authorization, even if that data is encrypted;

    c) Store any payment-related data that is not needed for business, legal, or regulatory purposes;

    d) Store payment verification code, payment verification value, or PIN verification value;

    e) Retain the primary account number unless retained n a manner consistent with the other requirements of this subdivision and in a form that is unreadable and unusable by unauthorized persons anywhere it is stored;

    f) Send payment-related data over open, public networks unless the data is encrypted using strong cryptography and security protocols or otherwise rendered indecipherable; and,

    g) Fail to limit access to payment-related data to only those individuals whose job requires that access.

2) Require that notification to the owner or licensee of the information to include, among other things, a description of the categories of personal information that were, or may have been, acquired, a toll-fee or local telephone number or e-mail address that individuals may use to contact the agency, person, or business, and the telephone numbers and addresses of the major credit reporting agencies. If the owner or licensee of the information is the issuer of the credit or debit card or the payment device, or maintains the account from which the payment device orders payment or is an agency required to give notice of a security breach as specified, the bill requires the owner or licensee to disclose the same information to the California resident in plain language, as specified.

3) Require, if substitute notice is utilized, that notice to also be provided to the Office of Information Security and Privacy Protection.

4) Specify that this bill only becomes operative if SB 364 (Simitian) is enacted and takes effect on or before January 1, 2009.

EXISTING LAW:

1) Requires businesses that own or license personal information about a California resident to implement and maintain reasonable security measures, disclose a breach of computerized data, and upon request, provide specified information to a customer in relation to the disclosure of personal information to third parties. For a violation of any of the above-described provisions, existing law allows an injured customer to institute a civil action to recover damages or for injunctive relief.

2) Requires any agency, person, or business that maintains computerized data that includes personal information that the agency, person, or business does not own, to notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonable believed to have been, acquired by an unauthorized person.

3) Requires any state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose any breach of the security of that data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. Allows for that disclosure by written notice, electronic notice, or, upon a specified condition, by substitute notice, which, if utilized, also requires notification to major statewide media.

AS PASSED BY THE ASSEMBLY, this bill required the California Department of Education to allocate funds to local education agencies and direct-funded charter schools in support of local data management activities.

FISCAL EFFECT: Unknown

COMMENTS: This bill generally prohibits businesses that accept credit and debit cards as forms of payment from storing, sending, or failing to limit access to a customer's payment related information, unless it is necessary for business, legal, or regulatory purposes. This bill would also require encryption or other security protocols when payment related data is sent over open, public networks. In addition, this bill seeks to strengthen the existing breach notification law by requiring that notices contain specified information and that notice also be provided to the Office of Information Security and Privacy Protection under certain circumstances.

This bill is a follow up to last year's AB 779 (Jones), which was prompted in part by several substantial and well-publicized examples of data breaches that compromised the payment-related data of millions of consumers, including credit card and debit card numbers. Although AB 779 passed out of both houses last year with overwhelming bipartisan support, that measure was vetoed by the Governor. In his veto message, the Governor stated:

> Protecting the personal information of every Californian is very important to me and I am committed to strong laws that safeguard every individual's privacy and prevent identity theft. Clearly, the need to protect personal information is increasingly critical as routine commercial transactions are more and more exclusively accomplished through electronic means.
>
> However, this bill attempts to legislate in an area where the marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers. In addition, the Payment Card Industry has already established minimum data security standards when storing, processing, or transmitting credit or debit cardholder information. This industry has the contractual ability to mandate the use of these standards, and is in a superior position to ensure that these standards keep up with changes in technology and the marketplace. This measure creates the potential for California law to be in conflict with private sector data security standards.
>
> While I support many of the provisions of this bill, it fails to provide clear definition of which business or agency "owns" or "licenses" data, and when that business or agency relinquishes legal responsibility as the owner or licensee. This issue and the data security requirements found in this bill will drive up the costs of compliance, particularly for small businesses.

The author contends that he has addressed the concerns raised in the veto message with amendments that, among other things, permit storage of data for the sole purpose of processing on-going and recurring payments, permit notices to contain a "date range" instead of an exact date of breach and discovery, and remove provisions that would have required the business that held that data at the time of breach to reimburse the financial institution for the costs of sending notification. It should be noted that the present bill adopts the underlying *concepts* of the private PCI standards referenced in the veto message, without legislating fixed standards. In addition, eliminating the reimbursement provisions that existed in last year's bill would seemingly assuage concerns about the relative responsibilities of "owners" and "licensees" of the data versus the entity that "maintained" the data at the time of the security breach.

It is not entirely clear whether these amendments will address all of the Governor's concerns, but the bill is substantially different from last year's AB 779 even as it seeks the same ends. One thing that is clear, however, is that the problem of data breaches has not abated. A recently issued report by the Identity Theft Resource Center found that more data breaches have been reported this year than in all of 2007. (*See* "Data Breaches Have Surpassed Level for All of '07, Report Finds," *available at* www.washingtonpost.com/wp-dyn/content/article/2008/08/25)

Writing in support of this measure, the bill's sponsor, the California Credit Union League, states:

> Under existing law, when a consumer provides their credit or debit card, or information, to a retailer, that retailer makes a unilateral decision whether or not they will store personal data without permission from the consumer. Also, the current system provides for no enforceable standards for the merchant to protect that stored data. Then, when a consumers' data is breached, the law shifts all financial burdens of that breach from consumer notification to card replacement to dealing with fraudulent transactions - onto

the card issuer. Adding insult to injury, the card issuer is prevented from even disclosing to the consumer where the breach took place or when!

Your AB 1656 would address the above inequitable system in important ways. First, the bill requires merchants and state agencies to better secure financial data they choose to retain - helping to limit opportunities for data breaches to occur. Second, your bill will provide consumers with more information about where and when data breaches are taking place - helping to create market pressure for merchants and state agencies to prevent data breaches.

AB 1656 represents a continuation of efforts begun in your AB 779 last year, and major points of concern with last year's bill have been addressed in this version. Specifically, a provision has been added to AB 1656 clarifying that merchants and state agencies may retain any information necessary to process recurring payments. In addition, you have taken an amendment to the bill allowing for disclosure of a broad date range during which a breach occurred, which some argue will help keep information on the success of specific hacking techniques away from criminals. You have removed language that some considered an invitation to litigation in defining what transaction authentication data a merchant or state agency may retain. And, most significant, you have dropped the reimbursement provisions in the bill that would have entitled financial institutions to reimbursement for the costs of replacing plastic card involved in a breach.

REGISTERED SUPPORT / OPPOSITION:

Support

California Credit Union League
California State Sheriff's Association
California Statewide Law Enforcement Association

Opposition

American Electronics Association
Association for Competitive Technology
AT&T
California Bankers Association
California Cable and Telecommunications Assn
California Chamber of Commerce
California Financial Services Association
California Grocers Association
California Independent Bankers
California Retailers Association
CTIA-The Wireless Association
EDS
Experian
First Data
Internet Alliance
National Business Coalition on E-Commerce and Privacy
NetChoice

Reed Elsevier
State Privacy and Security Coalition

Analysis Prepared by: Thomas Clark / JUD. / (916) 319-2334